FIG. 1

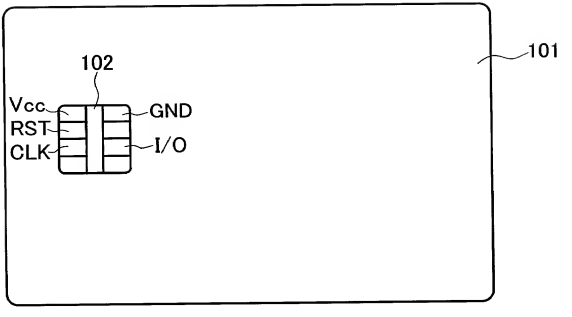
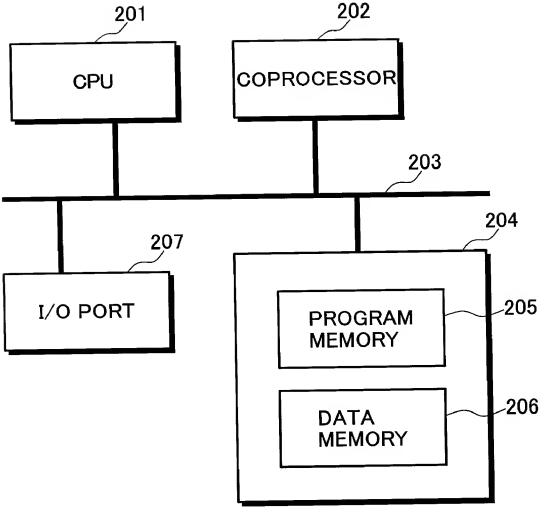
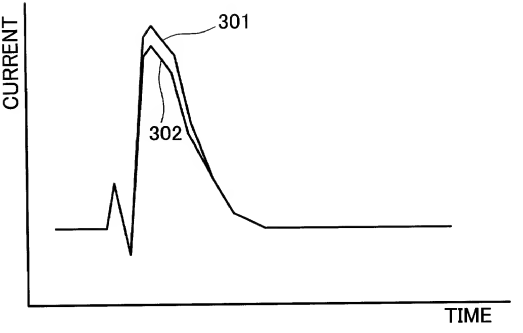


FIG. 2



JP06280-2804560

FIG. 3



US 6,280,286 B1

FIG. 4

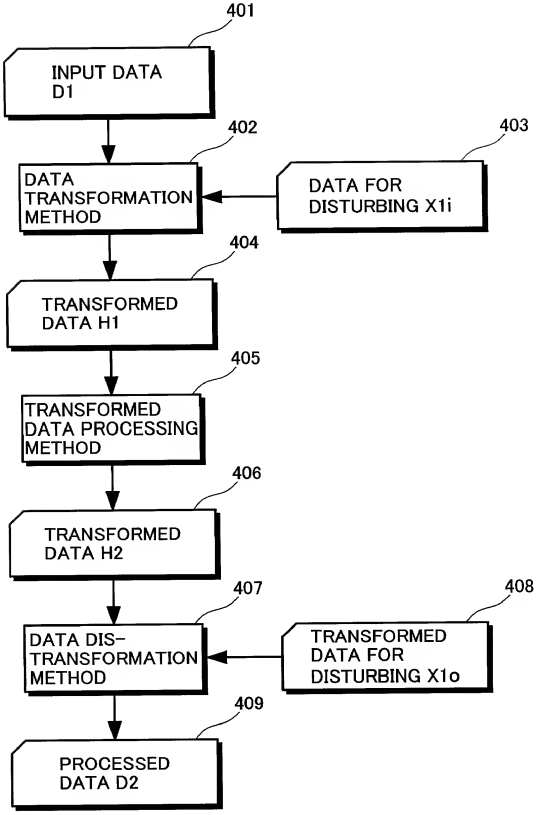
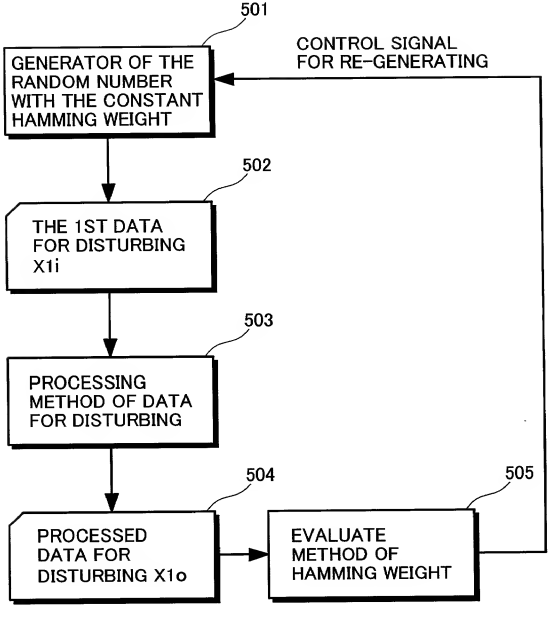
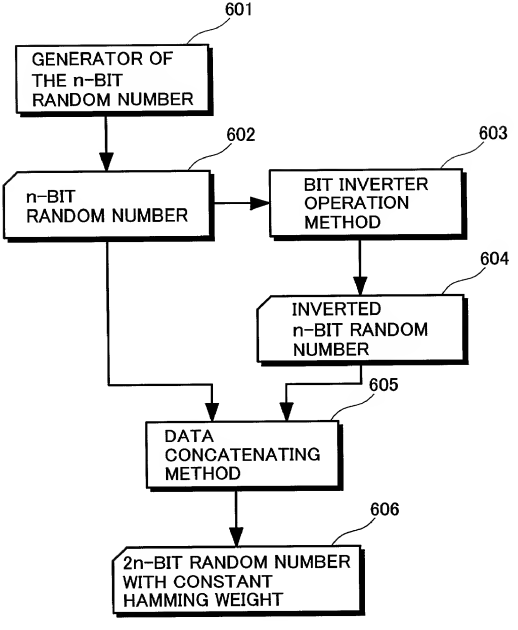

401
INPUT DATA D1
402
DATA TRANSFORMATION METHOD
403
DATA FOR DISTURBING X1i
404
TRANSFORMED DATA H1
405
TRANSFORMED DATA PROCESSING METHOD
406
TRANSFORMED DATA H2
407
DATA DIS-TRANSFORMATION METHOD
408
TRANSFORMED DATA FOR DISTURBING X1o
409
PROCESSED DATA D2

FIG. 5



TOKEN-2005040650

FIG. 6



US 2002/0080960

FIG. 7

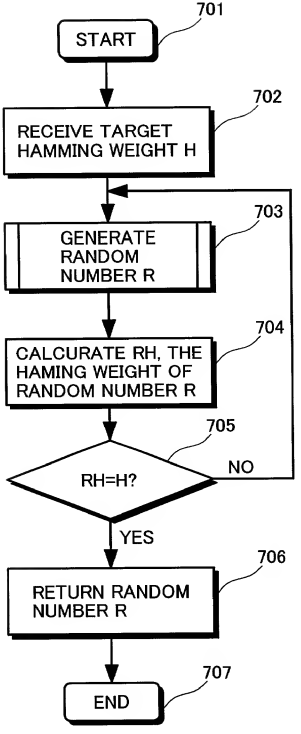

701
START
702
RECEIVE TARGET HAMMING WEIGHT H
703
GENERATE RANDOM NUMBER R
704
CALCURATE RH, THE HAMING WEIGHT OF RANDOM NUMBER R
705
RH=H?
NO
YES
706
RETURN RANDOM NUMBER R
707
END

FIG. 8

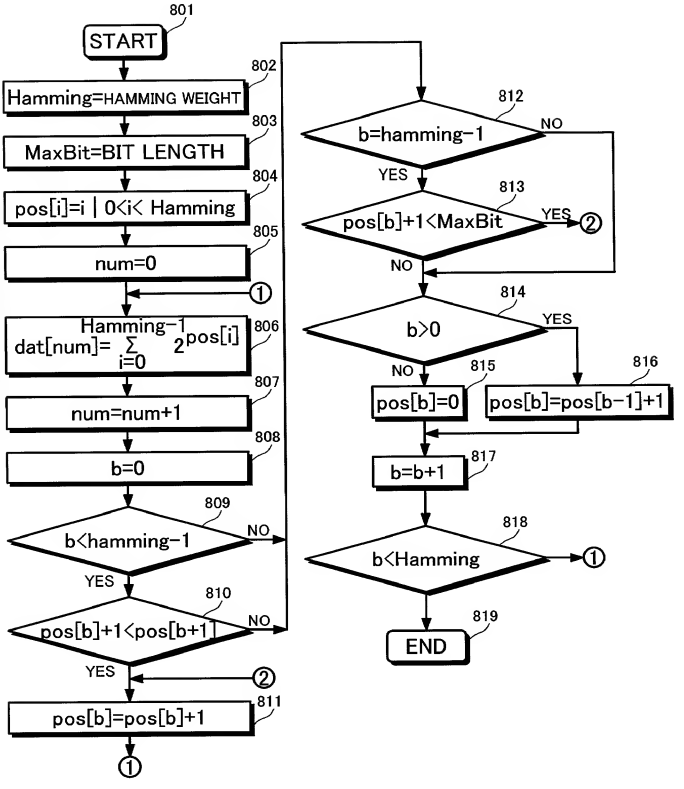

801
START
802
Hamming=HAMMING WEIGHT
803
MaxBit=BIT LENGTH
804
pos[i]=i | 0<i< Hamming
805
num=0
①
806
dat[num]= Σ 2^pos[i]
807
num=num+1
808
b=0
809
b<hamming-1
NO
YES
810
pos[b]+1<pos[b+1]
NO
YES
②
811
pos[b]=pos[b]+1
①
812
b=hamming-1
NO
YES
813
pos[b]+1<MaxBit
YES
②
NO
814
b>0
YES
NO
815
pos[b]=0
816
pos[b]=pos[b-1]+1
817
b=b+1
818
b<Hamming
①
819
END

FIG. 9

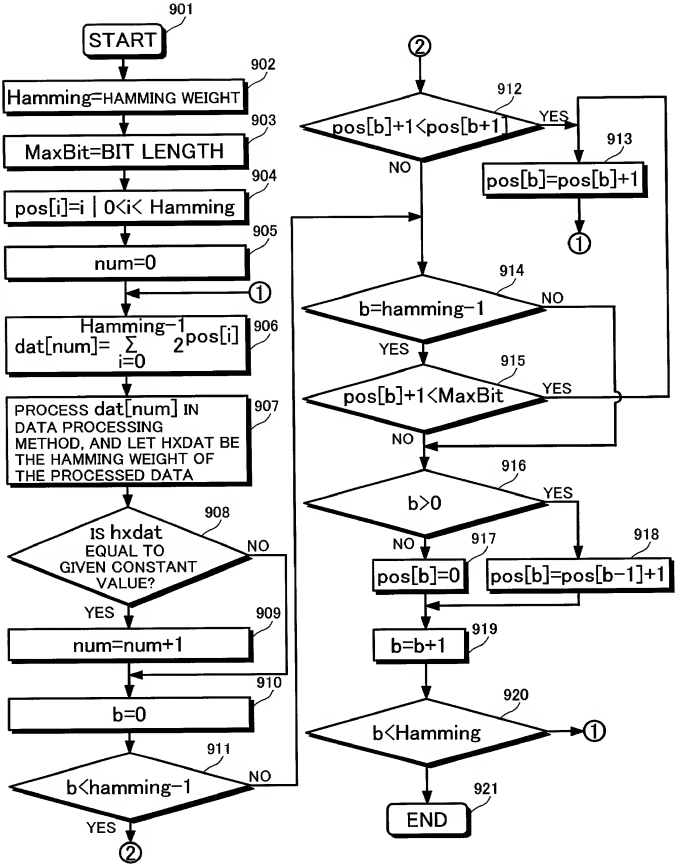

901
START
902
Hamming=HAMMING WEIGHT
903
MaxBit=BIT LENGTH
904
pos[i]=i | 0<i< Hamming
905
num=0
①
906
dat[num]= Σ 2^pos[i] (i=0 to Hamming−1)
907
PROCESS dat[num] IN DATA PROCESSING METHOD, AND LET HXDAT BE THE HAMMING WEIGHT OF THE PROCESSED DATA
908
IS hxdat EQUAL TO GIVEN CONSTANT VALUE?
NO
YES
909
num=num+1
910
b=0
911
b<hamming−1
NO
YES
②
②
912
pos[b]+1<pos[b+1]
YES
NO
913
pos[b]=pos[b]+1
①
914
b=hamming−1
NO
YES
915
pos[b]+1<MaxBit
YES
NO
916
b>0
YES
NO
917
pos[b]=0
918
pos[b]=pos[b−1]+1
919
b=b+1
920
b<Hamming
①
921
END

FIG. 10

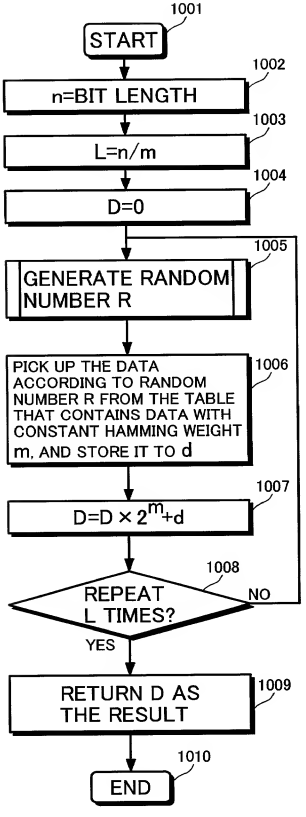

1001
START
1002
n=BIT LENGTH
1003
L=n/m
1004
D=0
1005
GENERATE RANDOM NUMBER R
1006
PICK UP THE DATA ACCORDING TO RANDOM NUMBER R FROM THE TABLE THAT CONTAINS DATA WITH CONSTANT HAMMING WEIGHT m, AND STORE IT TO d
1007
D=D × 2^m+d
1008
REPEAT L TIMES?
NO
YES
1009
RETURN D AS THE RESULT
1010
END

FIG. 11

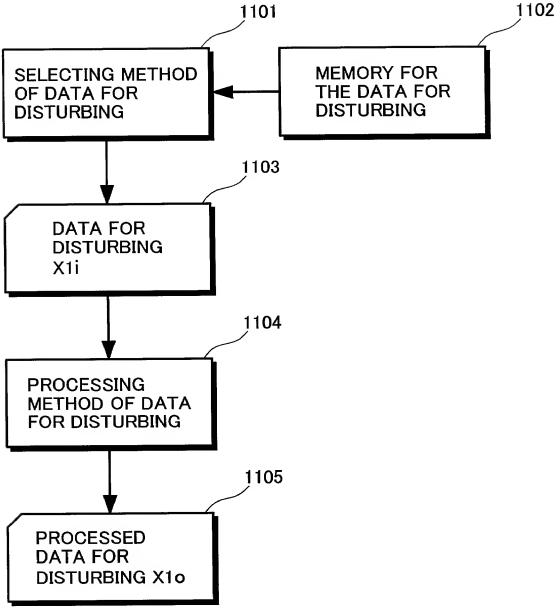
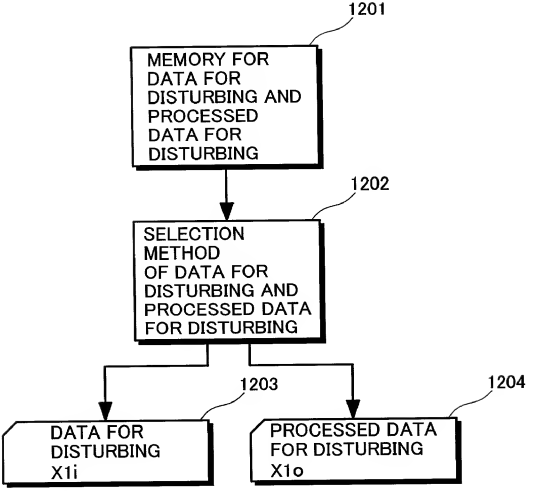
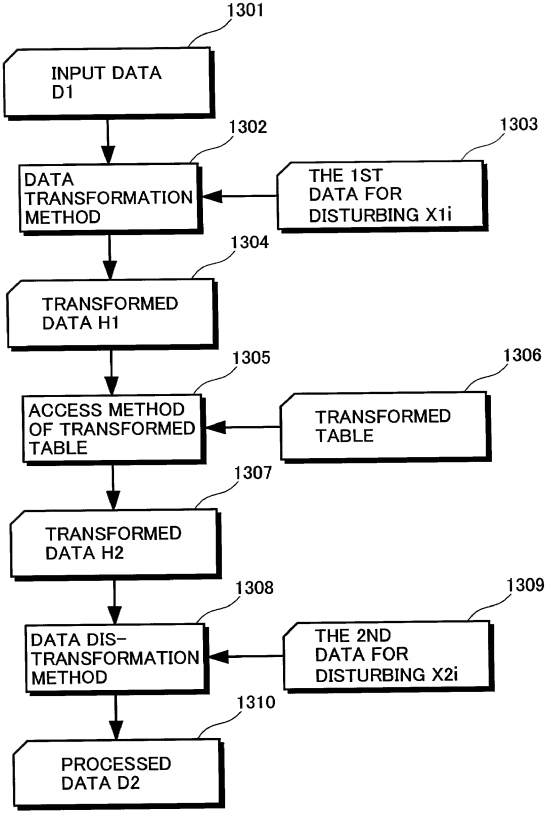

1101
1102
SELECTING METHOD OF DATA FOR DISTURBING
MEMORY FOR THE DATA FOR DISTURBING
1103
DATA FOR DISTURBING X1i
1104
PROCESSING METHOD OF DATA FOR DISTURBING
1105
PROCESSED DATA FOR DISTURBING X1o

FIG. 12



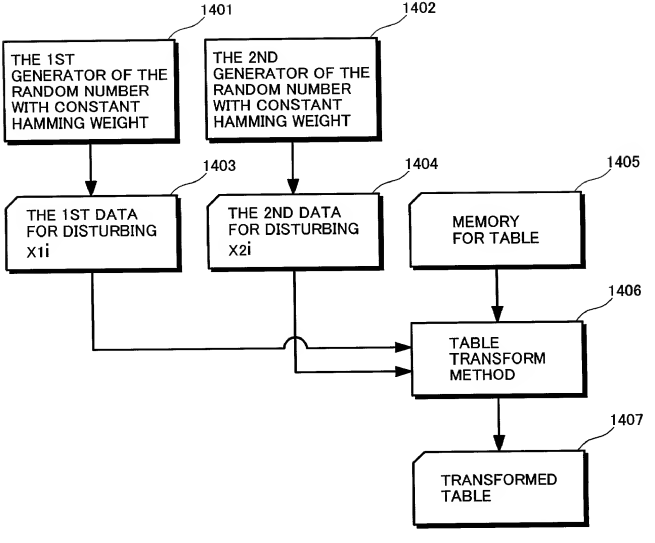
US 2006/0280286 A1

FIG. 13



10628 "2850660

FIG. 14



10/580,288 DOCKET

FIG. 15

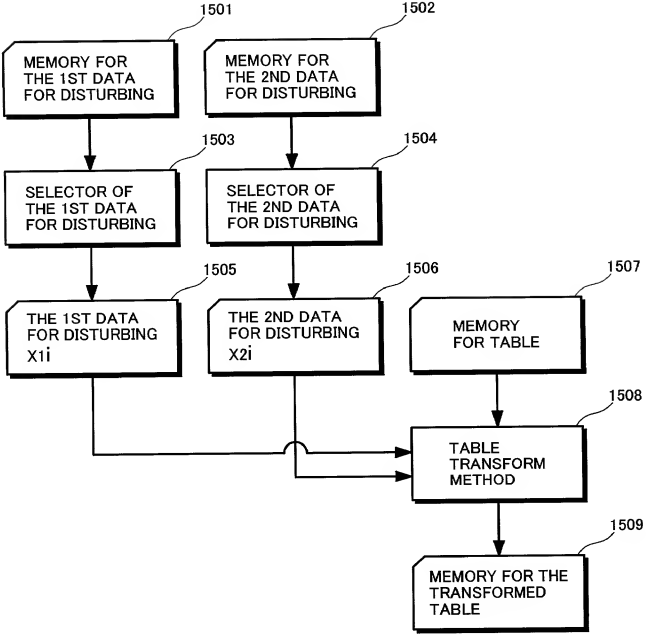

1501
MEMORY FOR THE 1ST DATA FOR DISTURBING
1502
MEMORY FOR THE 2ND DATA FOR DISTURBING
1503
SELECTOR OF THE 1ST DATA FOR DISTURBING
1504
SELECTOR OF THE 2ND DATA FOR DISTURBING
1505
THE 1ST DATA FOR DISTURBING X1i
1506
THE 2ND DATA FOR DISTURBING X2i
1507
MEMORY FOR TABLE
1508
TABLE TRANSFORM METHOD
1509
MEMORY FOR THE TRANSFORMED TABLE

FIG. 16

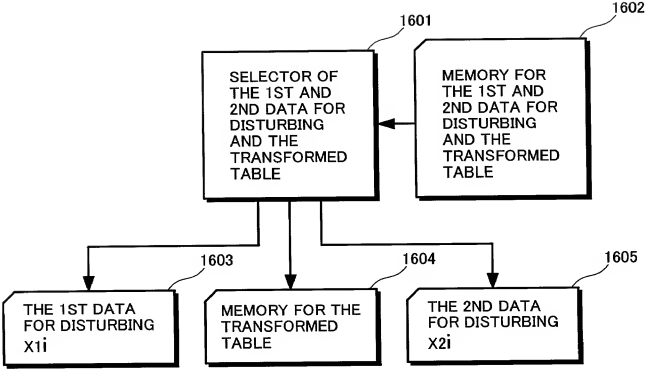

1601
1602
SELECTOR OF THE 1ST AND 2ND DATA FOR DISTURBING AND THE TRANSFORMED TABLE
MEMORY FOR THE 1ST AND 2ND DATA FOR DISTURBING AND THE TRANSFORMED TABLE
1603
1604
1605
THE 1ST DATA FOR DISTURBING X1i
MEMORY FOR THE TRANSFORMED TABLE
THE 2ND DATA FOR DISTURBING X2i

FIG. 17

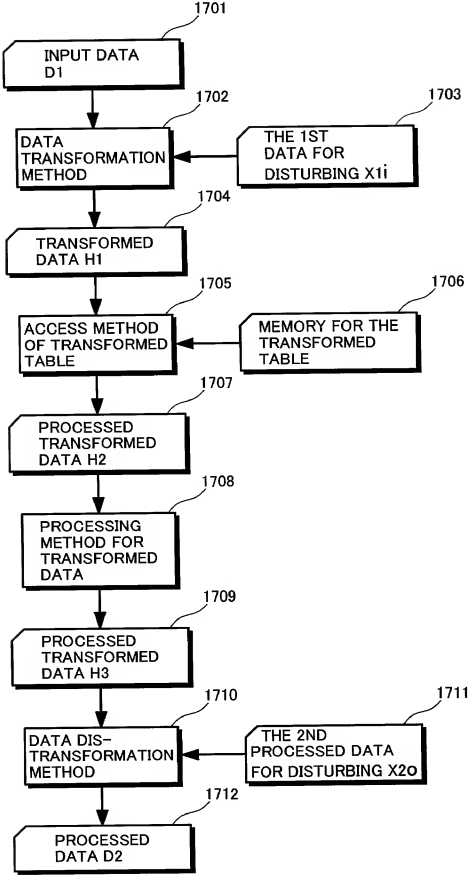

1701
INPUT DATA D1
1702
DATA TRANSFORMATION METHOD
1703
THE 1ST DATA FOR DISTURBING X1i
1704
TRANSFORMED DATA H1
1705
ACCESS METHOD OF TRANSFORMED TABLE
1706
MEMORY FOR THE TRANSFORMED TABLE
1707
PROCESSED TRANSFORMED DATA H2
1708
PROCESSING METHOD FOR TRANSFORMED DATA
1709
PROCESSED TRANSFORMED DATA H3
1710
DATA DIS-TRANSFORMATION METHOD
1711
THE 2ND PROCESSED DATA FOR DISTURBING X2o
1712
PROCESSED DATA D2

FIG. 18

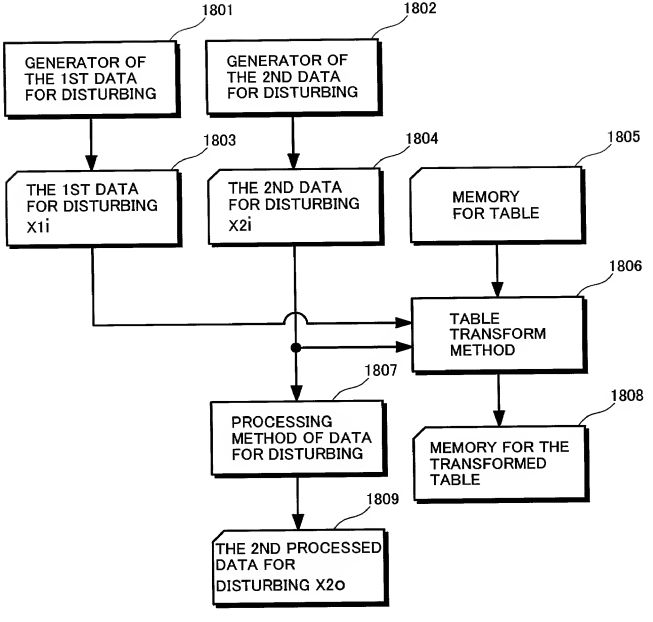

1801
GENERATOR OF THE 1ST DATA FOR DISTURBING
1802
GENERATOR OF THE 2ND DATA FOR DISTURBING
1803
THE 1ST DATA FOR DISTURBING X1i
1804
THE 2ND DATA FOR DISTURBING X2i
1805
MEMORY FOR TABLE
1806
TABLE TRANSFORM METHOD
1807
PROCESSING METHOD OF DATA FOR DISTURBING
1808
MEMORY FOR THE TRANSFORMED TABLE
1809
THE 2ND PROCESSED DATA FOR DISTURBING X2o

FIG. 19

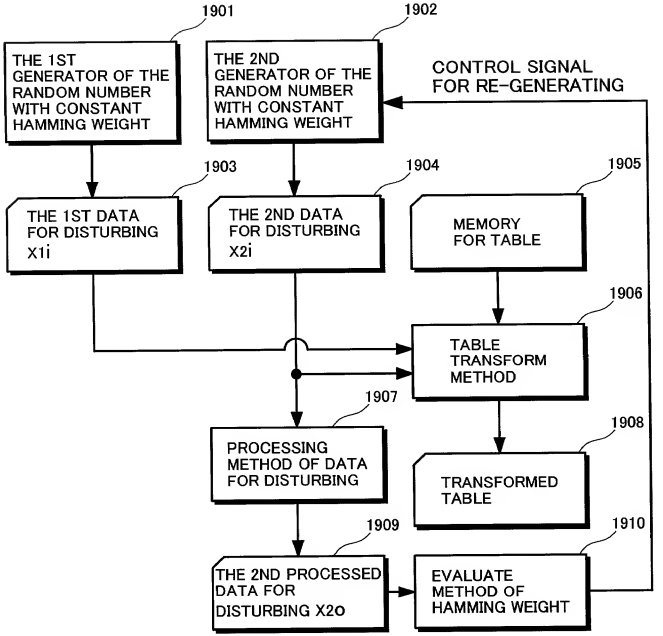
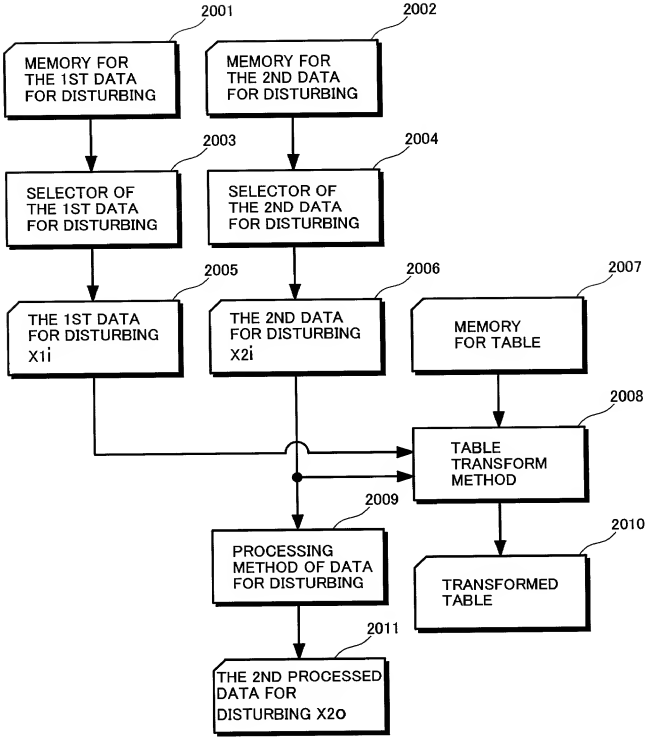

1901
1902
THE 1ST GENERATOR OF THE RANDOM NUMBER WITH CONSTANT HAMMING WEIGHT
THE 2ND GENERATOR OF THE RANDOM NUMBER WITH CONSTANT HAMMING WEIGHT
CONTROL SIGNAL FOR RE-GENERATING
1903
1904
1905
THE 1ST DATA FOR DISTURBING X1i
THE 2ND DATA FOR DISTURBING X2i
MEMORY FOR TABLE
1906
TABLE TRANSFORM METHOD
1907
1908
PROCESSING METHOD OF DATA FOR DISTURBING
TRANSFORMED TABLE
1909
1910
THE 2ND PROCESSED DATA FOR DISTURBING X2o
EVALUATE METHOD OF HAMMING WEIGHT

FIG. 20



0994058E2 · 082201

FIG. 21

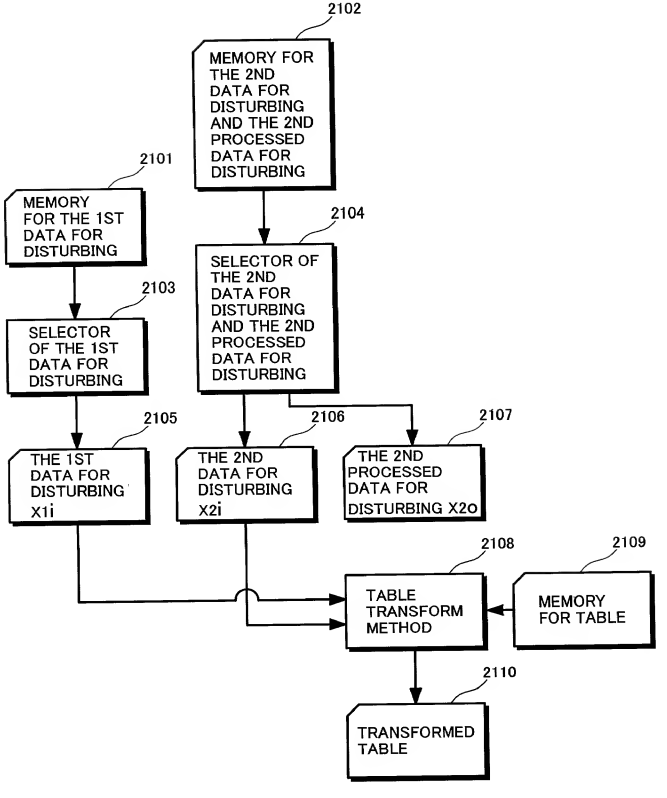
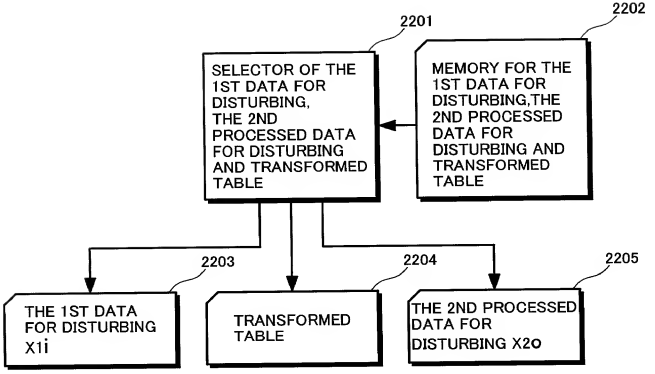
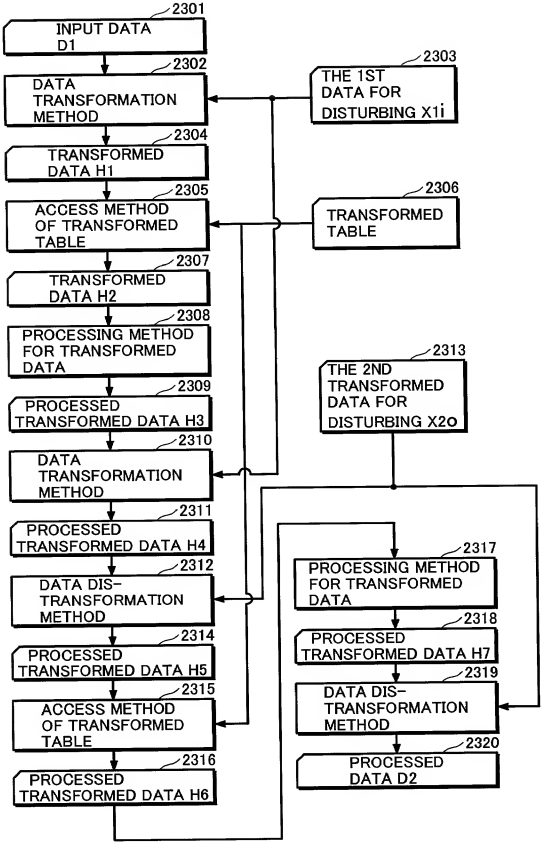

2102
MEMORY FOR THE 2ND DATA FOR DISTURBING AND THE 2ND PROCESSED DATA FOR DISTURBING
2101
MEMORY FOR THE 1ST DATA FOR DISTURBING
2104
SELECTOR OF THE 2ND DATA FOR DISTURBING AND THE 2ND PROCESSED DATA FOR DISTURBING
2103
SELECTOR OF THE 1ST DATA FOR DISTURBING
2105
THE 1ST DATA FOR DISTURBING X1i
2106
THE 2ND DATA FOR DISTURBING X2i
2107
THE 2ND PROCESSED DATA FOR DISTURBING X2o
2108
TABLE TRANSFORM METHOD
2109
MEMORY FOR TABLE
2110
TRANSFORMED TABLE

FIG. 22



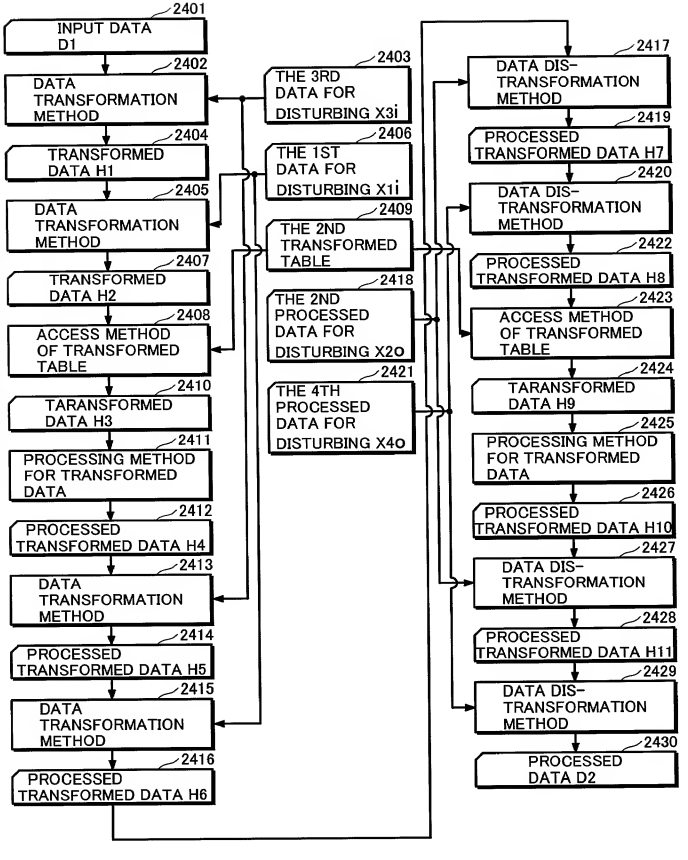
TW 200 * 2850 * 660

FIG. 23



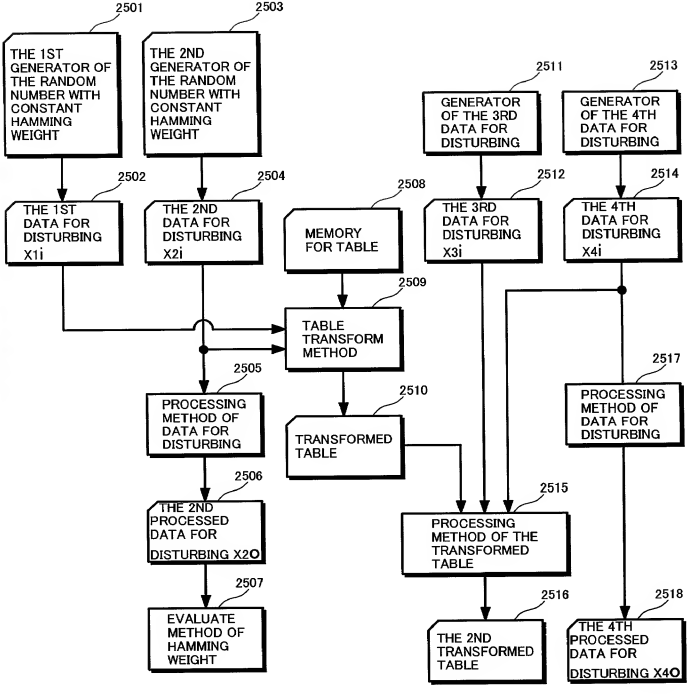
US 2002/0080961 A1

FIG. 24



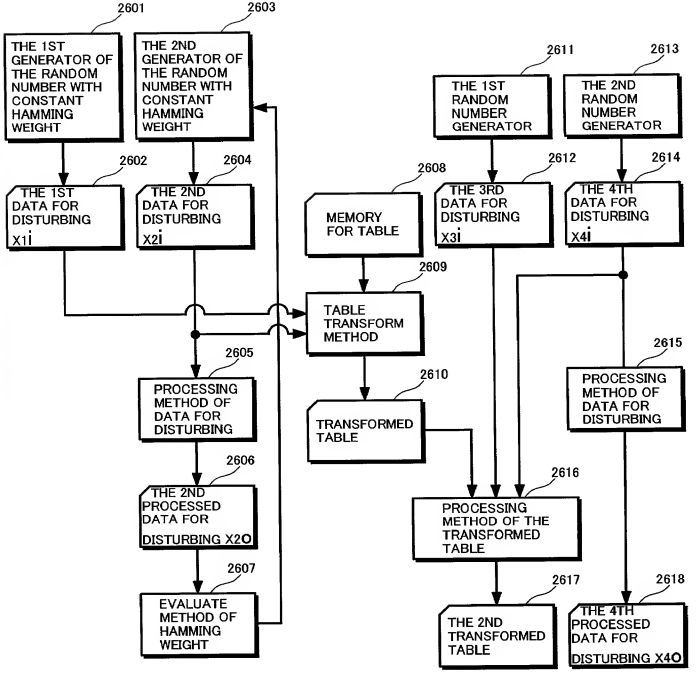
T06280*2860+650

FIG. 25



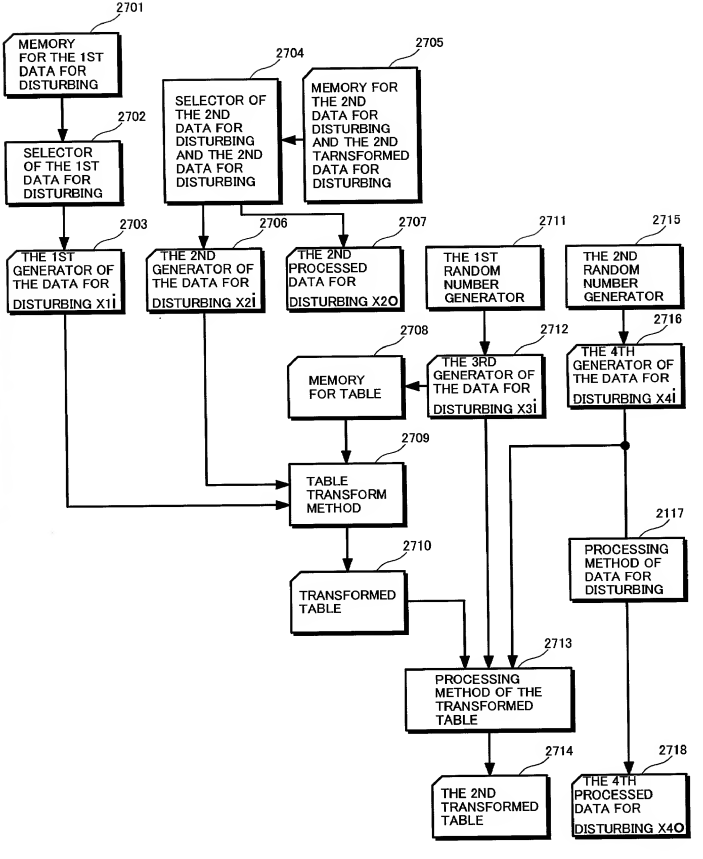
10/6280 - 2501+660

FIG. 26



US 2006/0269060 A1

FIG. 27



09280-2860-US

FIG. 28

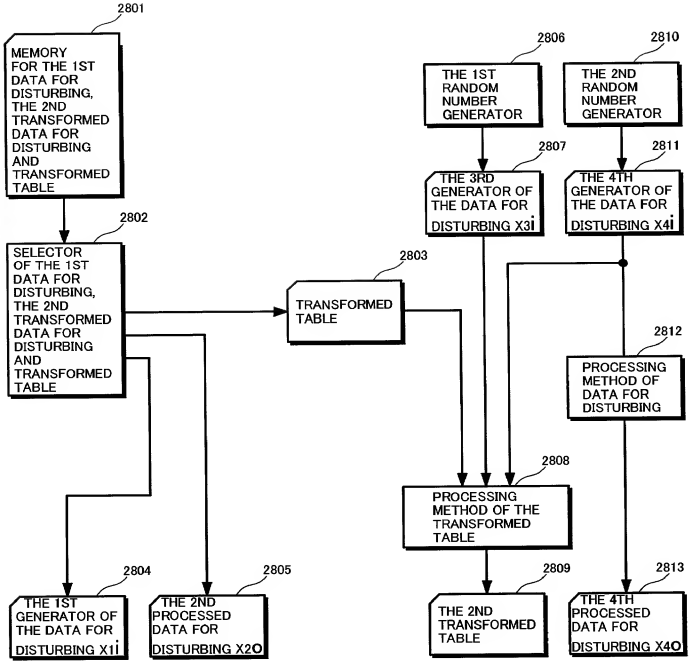
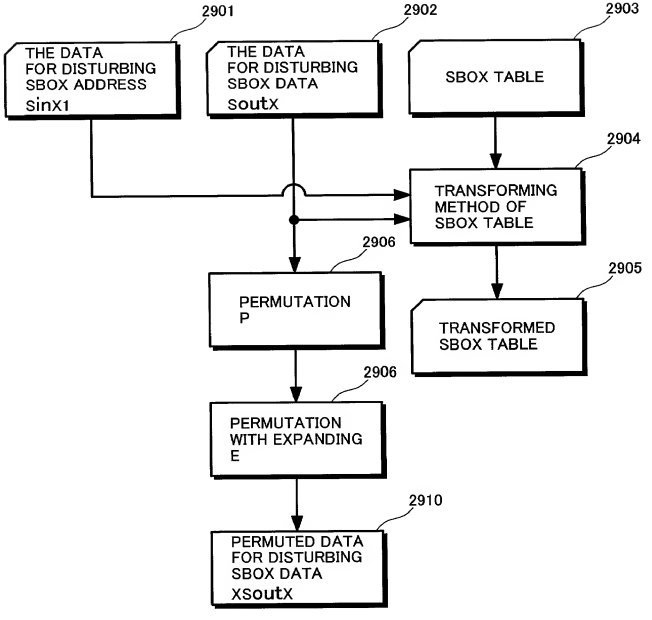
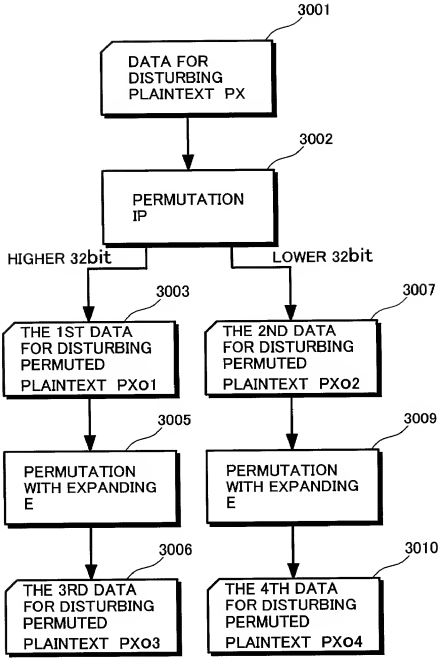

2801
MEMORY FOR THE 1ST DATA FOR DISTURBING, THE 2ND TRANSFORMED DATA FOR DISTURBING AND TRANSFORMED TABLE
2802
SELECTOR OF THE 1ST DATA FOR DISTURBING, THE 2ND TRANSFORMED DATA FOR DISTURBING AND TRANSFORMED TABLE
2803
TRANSFORMED TABLE
2804
THE 1ST GENERATOR OF THE DATA FOR DISTURBING X1i
2805
THE 2ND PROCESSED DATA FOR DISTURBING X2O
2806
THE 1ST RANDOM NUMBER GENERATOR
2807
THE 3RD GENERATOR OF THE DATA FOR DISTURBING X3i
2808
PROCESSING METHOD OF THE TRANSFORMED TABLE
2809
THE 2ND TRANSFORMED TABLE
2810
THE 2ND RANDOM NUMBER GENERATOR
2811
THE 4TH GENERATOR OF THE DATA FOR DISTURBING X4i
2812
PROCESSING METHOD OF DATA FOR DISTURBING
2813
THE 4TH PROCESSED DATA FOR DISTURBING X4O

FIG. 29



1062880 2860460

FIG. 30


3001
DATA FOR DISTURBING PLAINTEXT PX
3002
PERMUTATION IP
HIGHER 32bit
LOWER 32bit
3003
THE 1ST DATA FOR DISTURBING PERMUTED PLAINTEXT PX01
3007
THE 2ND DATA FOR DISTURBING PERMUTED PLAINTEXT PX02
3005
PERMUTATION WITH EXPANDING E
3009
PERMUTATION WITH EXPANDING E
3006
THE 3RD DATA FOR DISTURBING PERMUTED PLAINTEXT PX03
3010
THE 4TH DATA FOR DISTURBING PERMUTED PLAINTEXT PX04

1092280-2604660

FIG. 31

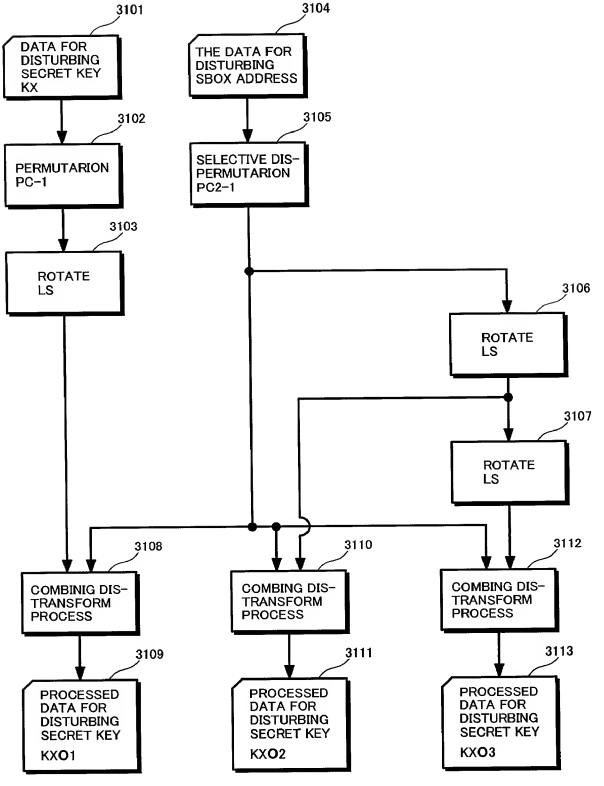
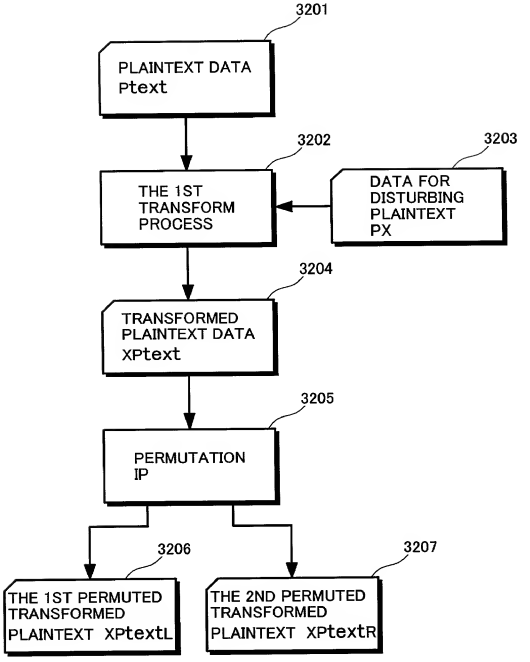
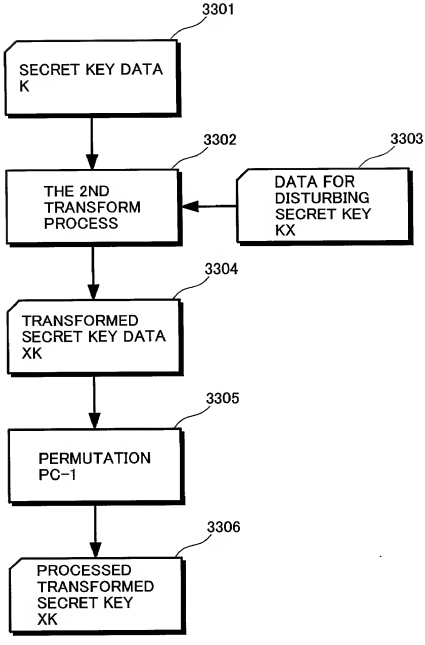


FIG. 32



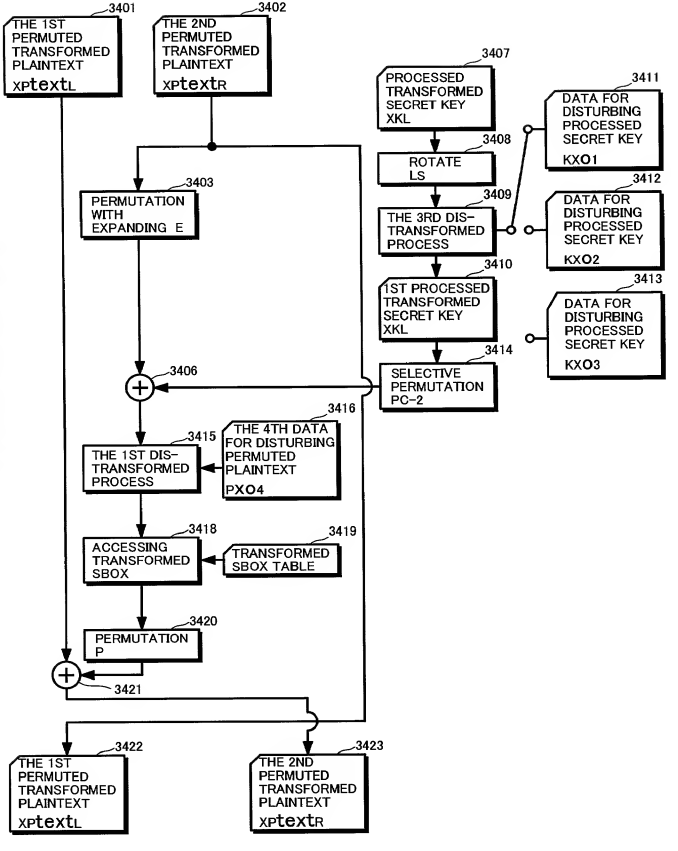
106280.2850450

FIG. 33



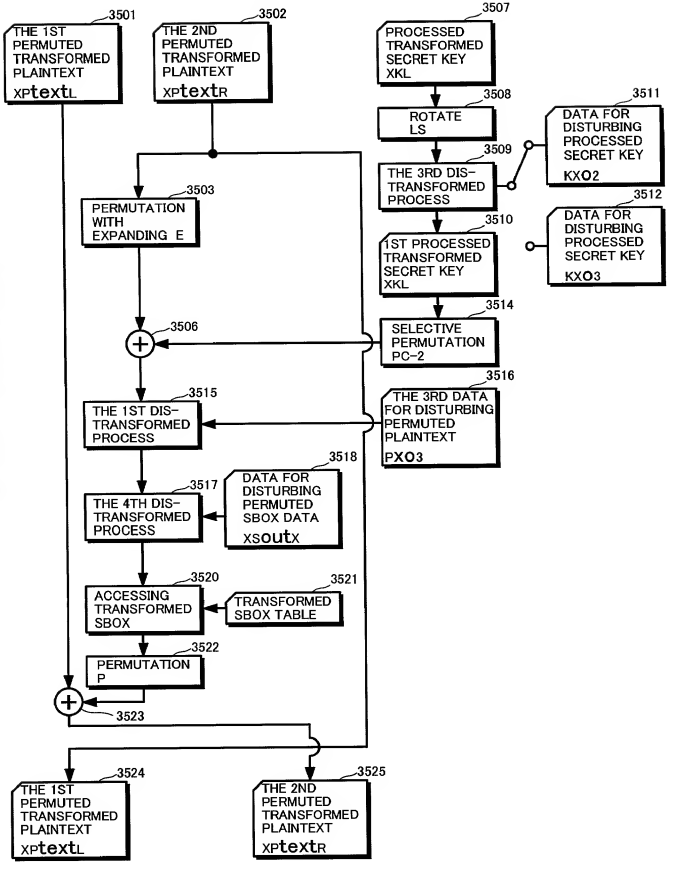
EP 0 862 290 A2

FIG. 34



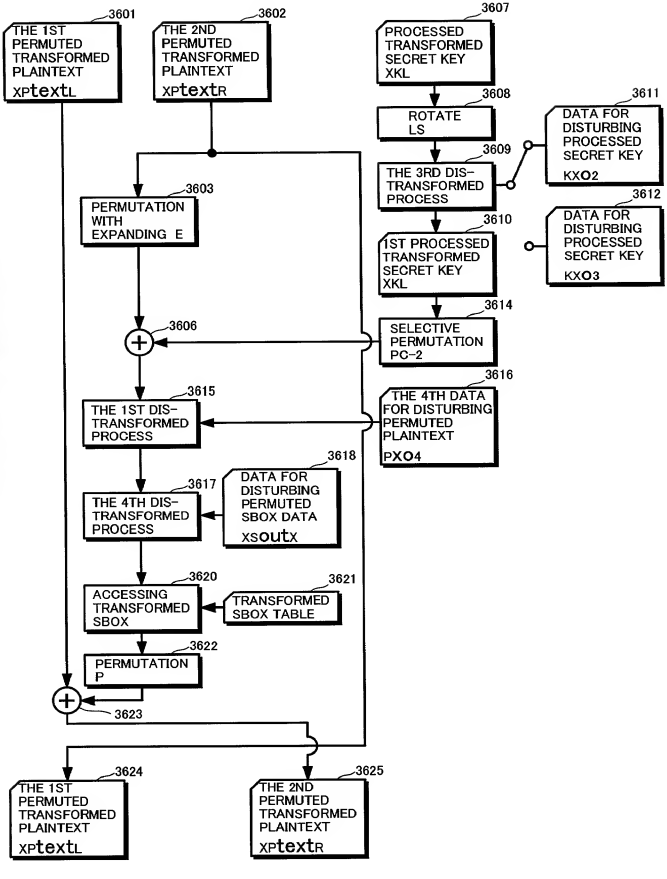
EP 2 860 700 A1

FIG. 35



"EP 2 063 420 A1"

FIG. 36



US 6,266,409 B1

FIG. 37

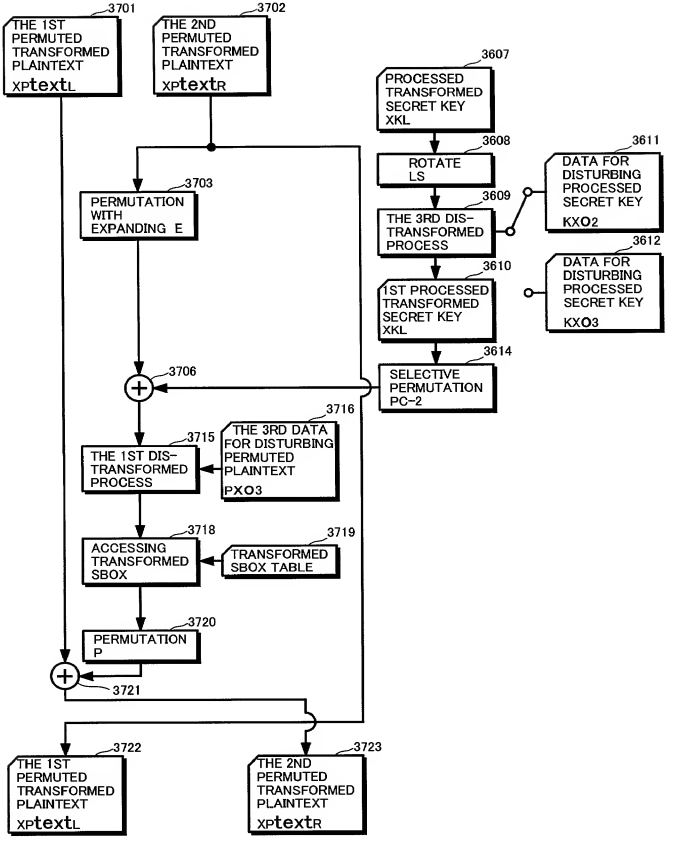

3701
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
3702
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR
3607
PROCESSED TRANSFORMED SECRET KEY
XKL
3608
ROTATE LS
3611
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO2
3609
THE 3RD DIS-TRANSFORMED PROCESS
3612
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO3
3610
1ST PROCESSED TRANSFORMED SECRET KEY
XKL
3614
SELECTIVE PERMUTATION
PC-2
3703
PERMUTATION WITH EXPANDING E
3706
3716
THE 3RD DATA FOR DISTURBING PERMUTED PLAINTEXT
PXO3
3715
THE 1ST DIS-TRANSFORMED PROCESS
3718
ACCESSING TRANSFORMED SBOX
3719
TRANSFORMED SBOX TABLE
3720
PERMUTATION
P
3721
3722
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
3723
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR

FIG. 38

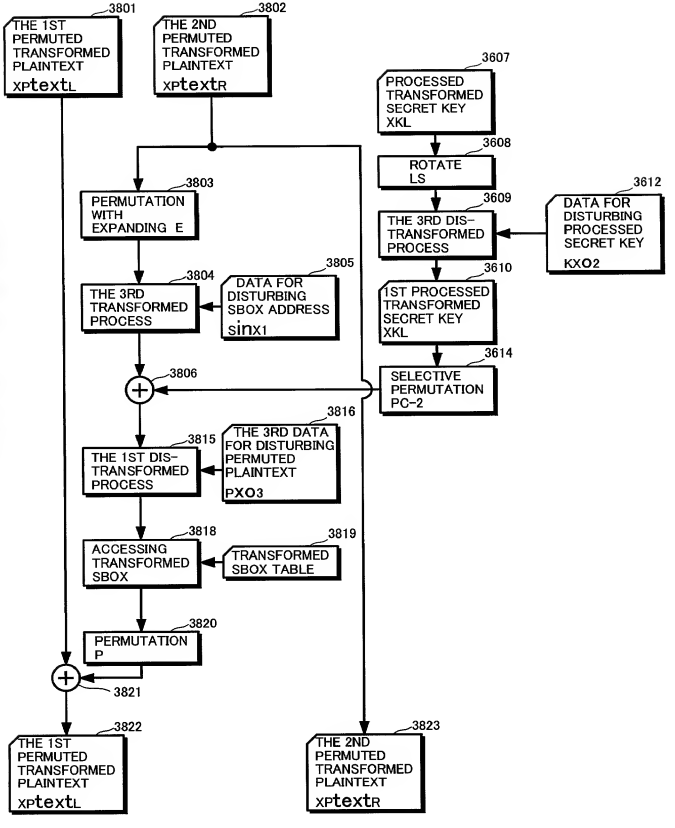
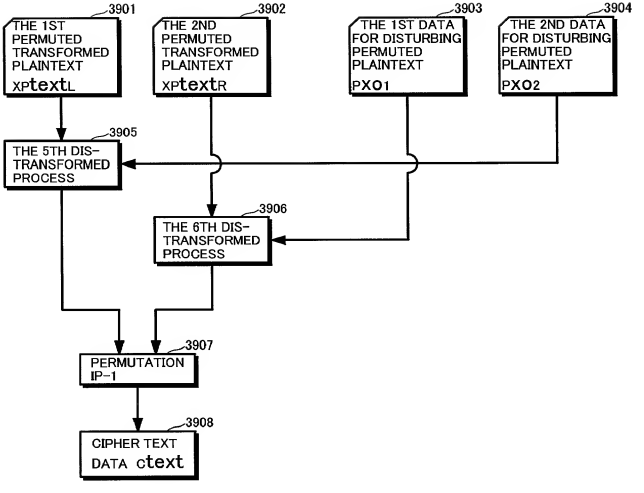
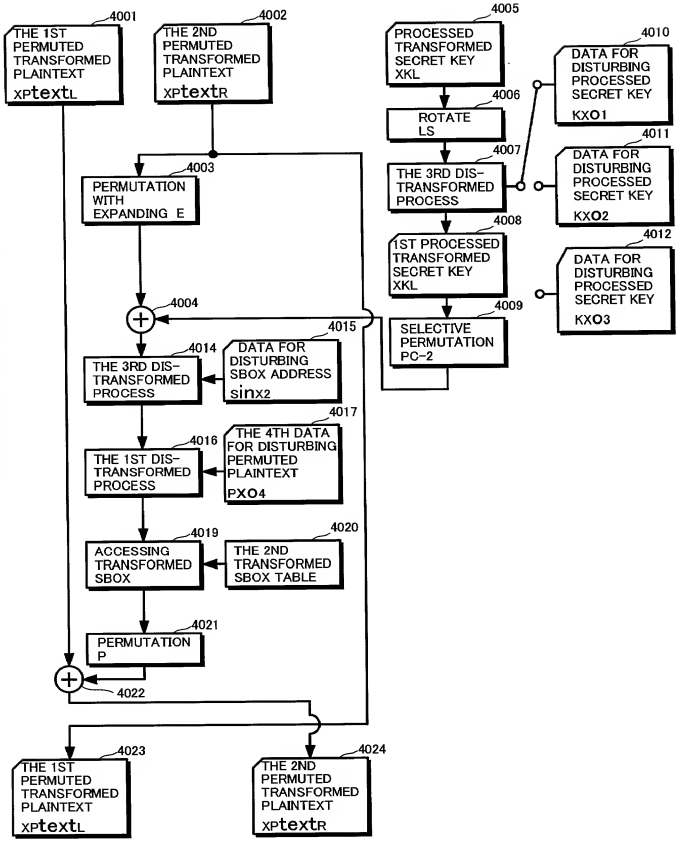

3801
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
3802
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR
3607
PROCESSED TRANSFORMED SECRET KEY
XKL
3608
ROTATE
LS
3612
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO2
3609
THE 3RD DIS-TRANSFORMED PROCESS
3610
1ST PROCESSED TRANSFORMED SECRET KEY
XKL
3614
SELECTIVE PERMUTATION
PC-2
3803
PERMUTATION WITH EXPANDING E
3804
THE 3RD TRANSFORMED PROCESS
3805
DATA FOR DISTURBING SBOX ADDRESS
sinX1
3806
3816
THE 3RD DATA FOR DISTURBING PERMUTED PLAINTEXT
PXO3
3815
THE 1ST DIS-TRANSFORMED PROCESS
3818
ACCESSING TRANSFORMED SBOX
3819
TRANSFORMED SBOX TABLE
3820
PERMUTATION
P
3821
3822
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
3823
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR

FIG. 39



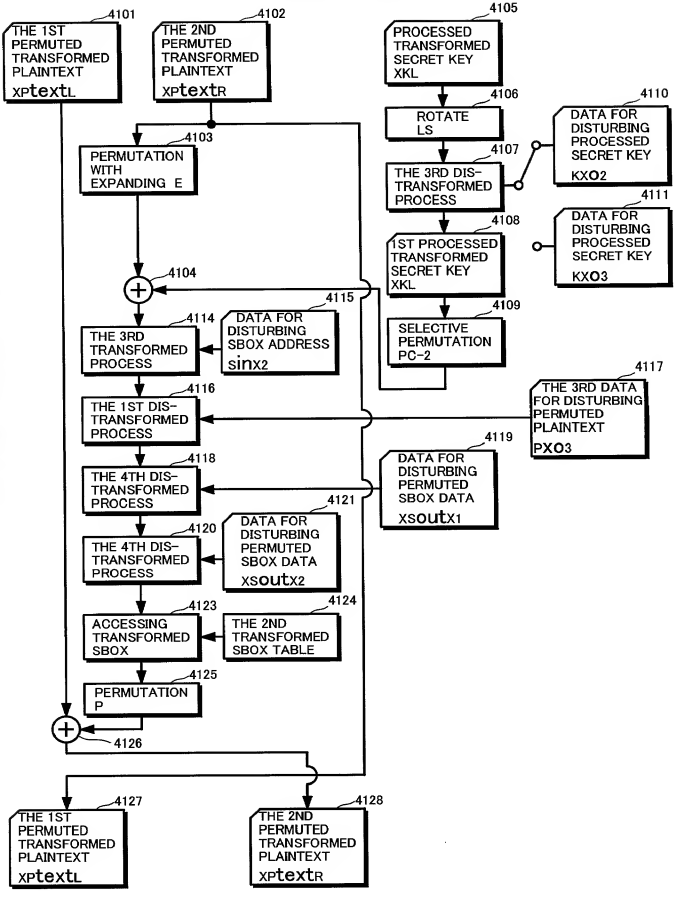
EP 1 062 280 B1 2005-08-24

FIG. 40



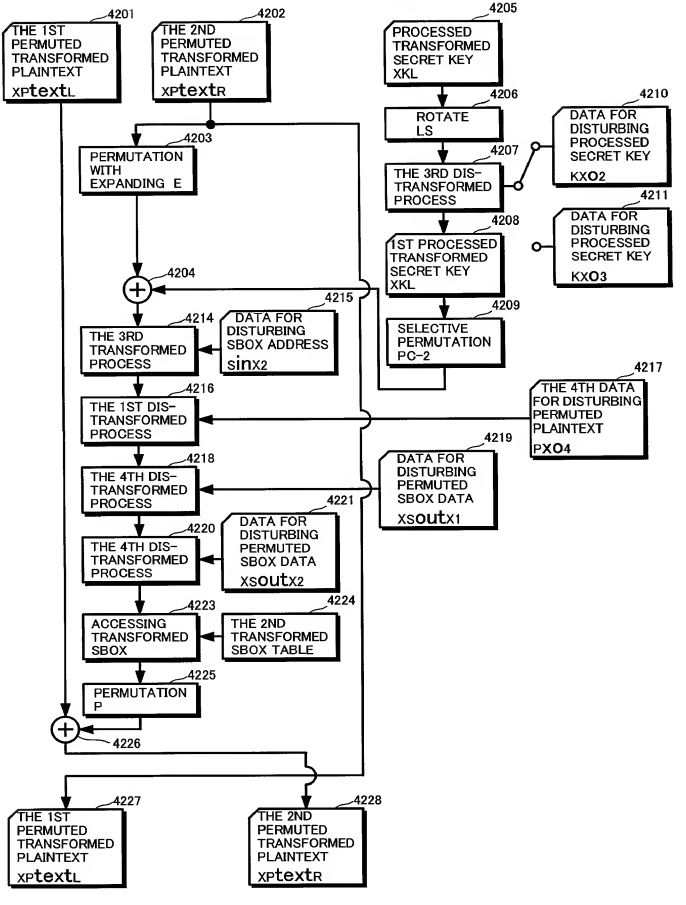
EP 0 982 980 A2

FIG. 41



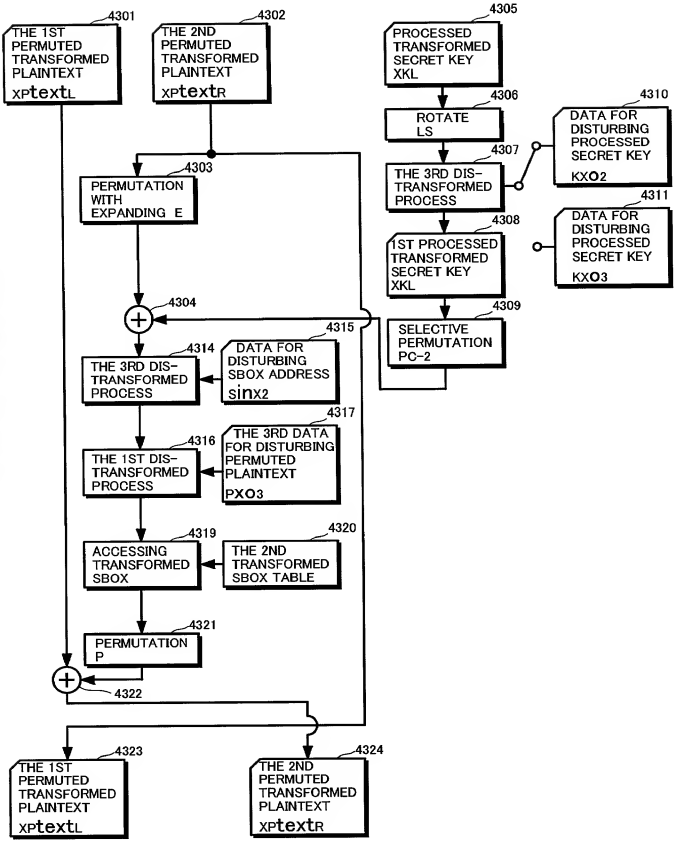
T05280*2850H660

FIG. 42



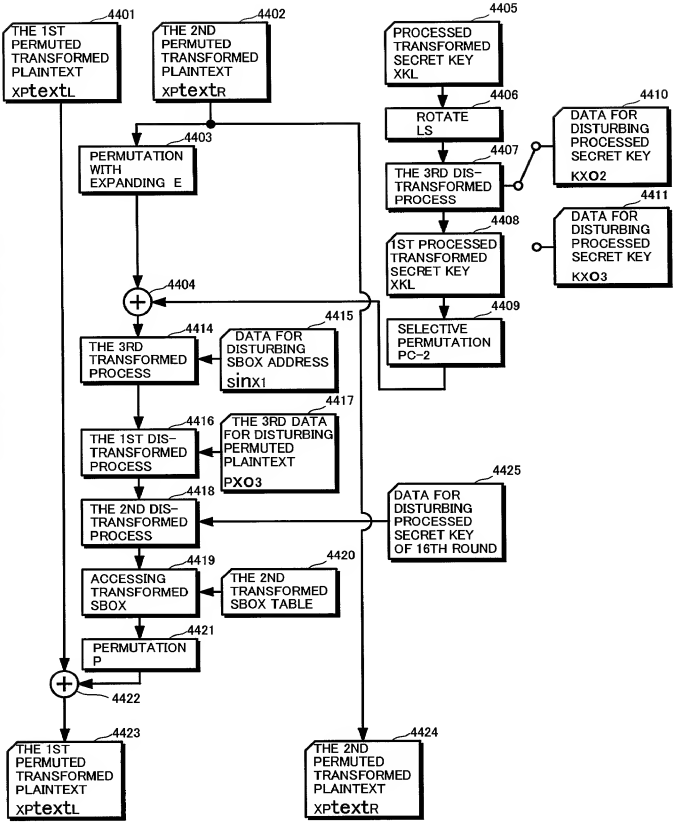
T06380*2860660

FIG. 43



"10290" 2860660

FIG. 44



US 6,266,780 B1 Jul. 24, 2001

FIG. 45

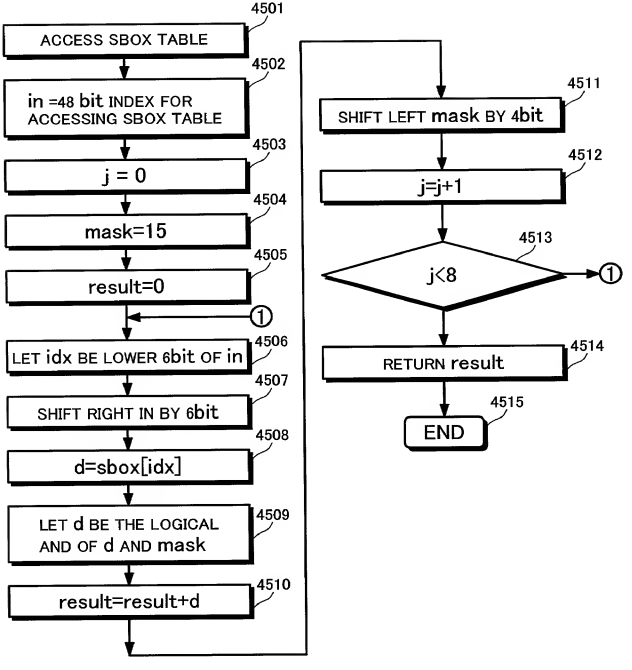

4501
ACCESS SBOX TABLE
4502
in =48 bit INDEX FOR ACCESSING SBOX TABLE
4503
j = 0
4504
mask=15
4505
result=0
1
4506
LET idx BE LOWER 6bit OF in
4507
SHIFT RIGHT IN BY 6bit
4508
d=sbox[idx]
4509
LET d BE THE LOGICAL AND OF d AND mask
4510
result=result+d
4511
SHIFT LEFT mask BY 4bit
4512
j=j+1
4513
j<8
1
4514
RETURN result
4515
END

FIG. 46

INDEX	VALUE	INDEX	VALUE	INDEX	VALUE	INDEX	VALUE
0	0XEFA72CAD	16	0X3911803A	32	0X40DA4917	48	0XF5BFF7A0
1	0X03DDEAD1	17	0XAC2456EC	33	0XFD13B462	49	0X5B496B9F
2	0X410DC1B2	18	0XA7D25DC9	34	0X1E662E4B	50	0XC81190F6
3	0XFD78BF0F	19	0X60870135	35	0XC8AF83B1	51	0XB6F4FE5C
4	0XD89E4A28	20	0X62C83393	36	0XE7491FB4	52	0X9C23C46A
5	0X740B24BD	21	0XC152FD56	37	0X8AD0C2DE	53	0X37E50109
6	0X1EE31FE4	22	0XCD75F47E	38	0X8B90B5D1	54	0X76CE5A8D
7	0X4795C278	23	0XBAECAECB	39	0X21067C87	55	0XEC3B97F0
8	0X266079F6	24	0X5CBBDE55	40	0XDA8CA2C9	56	0X3955610F
9	0XEF36474A	25	0X96C13020	41	0X436A1914	57	0XA0BCA6E3
10	0XFB36A20F	26	0X904C07A0	42	0X64FBD83C	58	0XA3A23D53
11	0X224F7C93	27	0X59BA9BFE	43	0X9F91E54A	59	0X05574025
12	0XB3F9B68B	28	0X0524E56C	44	0X2D377C7E	60	0X52E80B95
13	0XD860D917	29	0X3BFE8389	45	0X148D2FA8	61	0X6E225836
14	0X845A68D1	30	0X7A8F9817	46	0XB10D83E2	62	0X0F74E628
15	0X1EA315A4	31	0X85196862	47	0X7278DA7D	63	0XD9CE3DCB

FIG. 47

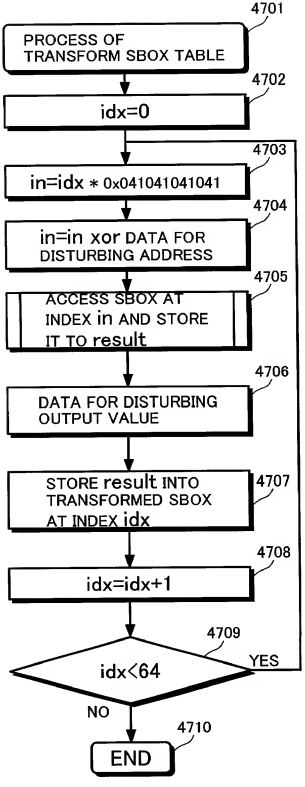

4701
PROCESS OF TRANSFORM SBOX TABLE
4702
idx=0
4703
in=idx * 0x041041041041
4704
in=in xor DATA FOR DISTURBING ADDRESS
4705
ACCESS SBOX AT INDEX in AND STORE IT TO result
4706
DATA FOR DISTURBING OUTPUT VALUE
4707
STORE result INTO TRANSFORMED SBOX AT INDEX idx
4708
idx=idx+1
4709
idx<64
YES
NO
4710
END

FIG. 48

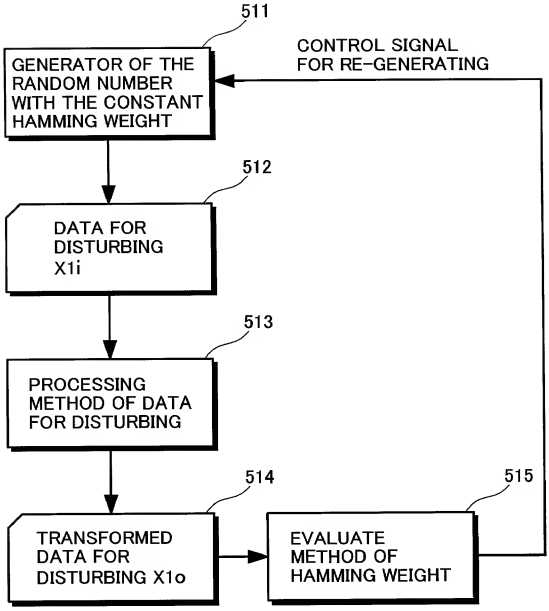
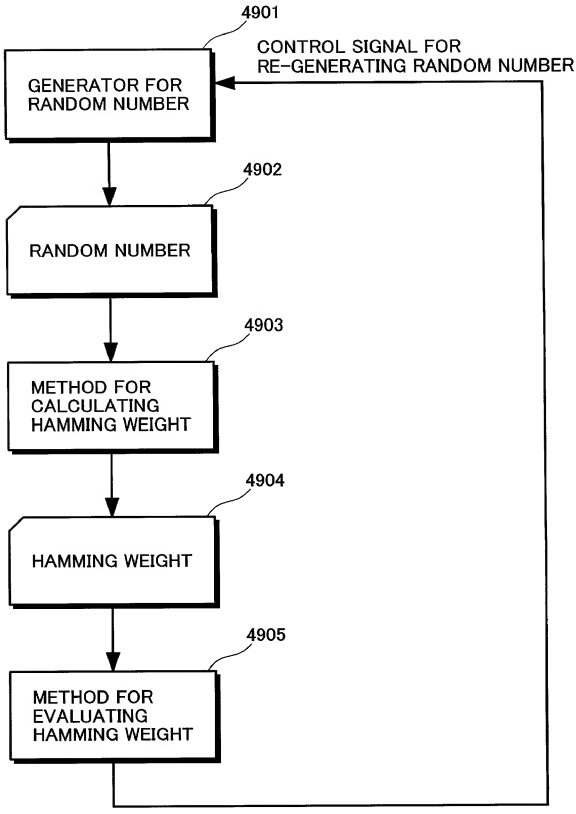
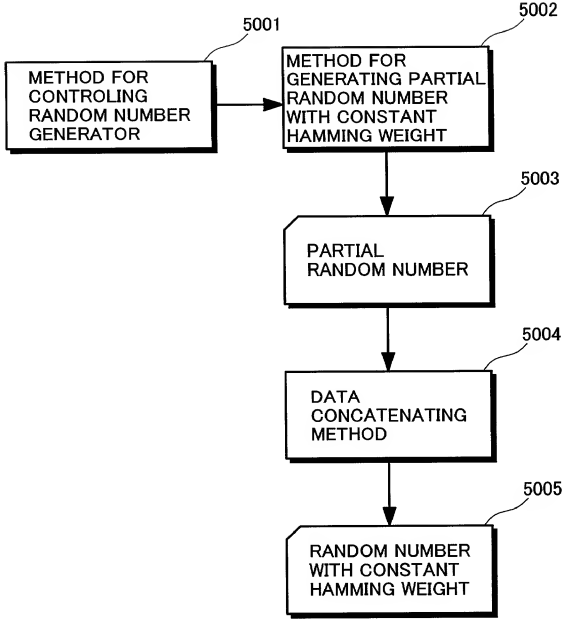

511
GENERATOR OF THE RANDOM NUMBER WITH THE CONSTANT HAMMING WEIGHT
CONTROL SIGNAL FOR RE-GENERATING
512
DATA FOR DISTURBING X1i
513
PROCESSING METHOD OF DATA FOR DISTURBING
514
TRANSFORMED DATA FOR DISTURBING X1o
515
EVALUATE METHOD OF HAMMING WEIGHT

FIG. 49



TD9280'28604950

FIG. 50



1062820.2860660

FIG. 51

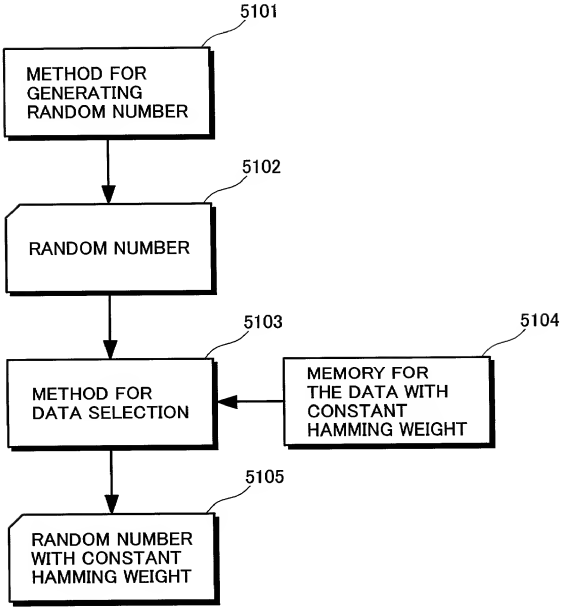

5101
METHOD FOR GENERATING RANDOM NUMBER
5102
RANDOM NUMBER
5103
METHOD FOR DATA SELECTION
5104
MEMORY FOR THE DATA WITH CONSTANT HAMMING WEIGHT
5105
RANDOM NUMBER WITH CONSTANT HAMMING WEIGHT

FIG. 52

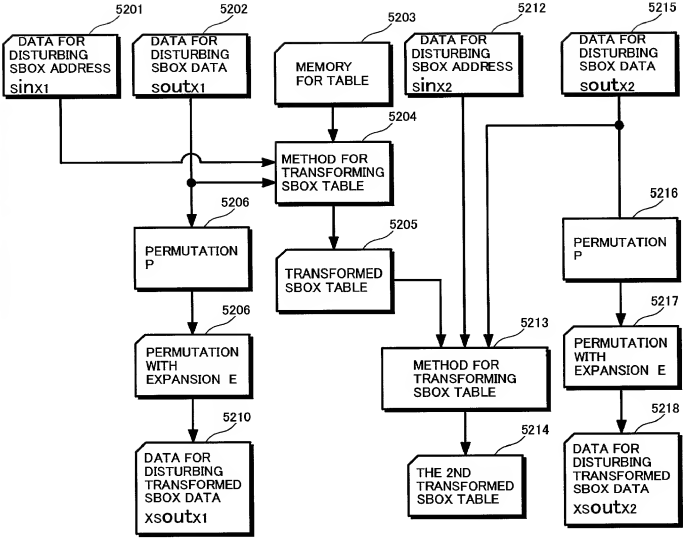
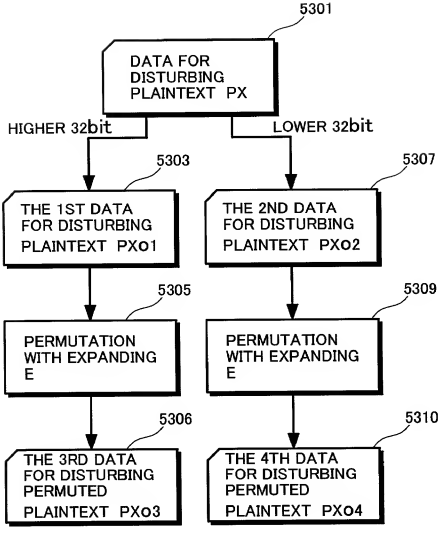

5201
DATA FOR DISTURBING SBOX ADDRESS sinx1
5202
DATA FOR DISTURBING SBOX DATA soutx1
5203
MEMORY FOR TABLE
5212
DATA FOR DISTURBING SBOX ADDRESS sinx2
5215
DATA FOR DISTURBING SBOX DATA soutx2
5204
METHOD FOR TRANSFORMING SBOX TABLE
5206
PERMUTATION P
5205
TRANSFORMED SBOX TABLE
5216
PERMUTATION P
5206
PERMUTATION WITH EXPANSION E
5213
METHOD FOR TRANSFORMING SBOX TABLE
5217
PERMUTATION WITH EXPANSION E
5210
DATA FOR DISTURBING TRANSFORMED SBOX DATA xsoutx1
5214
THE 2ND TRANSFORMED SBOX TABLE
5218
DATA FOR DISTURBING TRANSFORMED SBOX DATA xsoutx2

FIG. 53



106280.2850465.0

FIG. 54

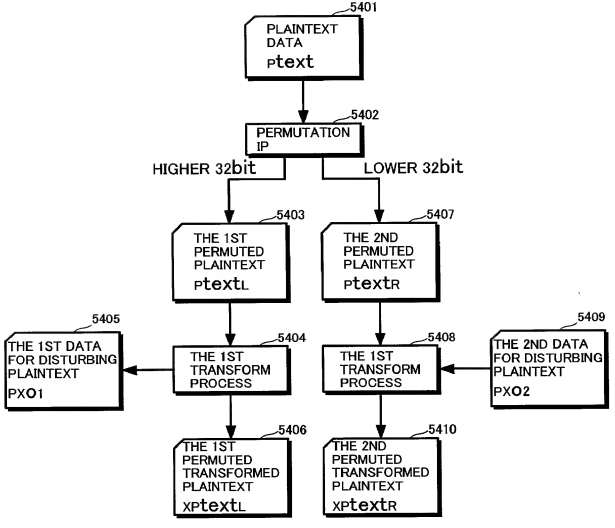

5401
PLAINTEXT DATA
Ptext
5402
PERMUTATION IP
HIGHER 32bit
LOWER 32bit
5403
THE 1ST PERMUTED PLAINTEXT
PtextL
5407
THE 2ND PERMUTED PLAINTEXT
PtextR
5405
THE 1ST DATA FOR DISTURBING PLAINTEXT
PXO1
5404
THE 1ST TRANSFORM PROCESS
5408
THE 1ST TRANSFORM PROCESS
5409
THE 2ND DATA FOR DISTURBING PLAINTEXT
PXO2
5406
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
5410
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR

FIG. 55

IN THE CASE OF LEFT ROTATION

1201

X1i	X1o
0X55555555	0xaaaaaaaa
0X33333333	0X66666666
0X66666666	0Xcccccccc

FIG. 56

1501

THE 1ST DATA FOR DISTURBING
0X1C71C71C71C7
0x38e38e38e38e
0x34d34d34d34d
0x2cb2cb2cb2cb
0X38e38e38e38e

1502

THE 2ND DATA FOR DISTURBING
0X55555555
0XAAAAAAAA
0XOFOFOFOF
0X71717171
0X5a5a5a5a

FIG. 57

IN THE CASE OF

THE 1ST DATA FOR DISTURBING=0x1c71c71c71c7
THE 2ND DATA FOR DISTURBING=0x55555555

1507

INDEX	VALUE	INDEX	VALUE	INDEX	VALUE	INDEX	VALUE
0	0XEFA72CAD	16	0X3911803A	32	0X40DA4917	48	0XF5BFF7A0
1	0X03DDEAD1	17	0XAC2456EC	33	0XFD13B462	49	0X5B496B9F
2	0X410DC1B2	18	0XA7D25DC9	34	0X1E662E4B	50	0XC81190F6
3	0XFD78BF0F	19	0X60870135	35	0XC8AF83B1	51	0XB6F4FE5C
4	0XD89E4A28	20	0X62C83393	36	0XE7491FB4	52	0X9C23C46A
5	0X740B24BD	21	0XC152FD56	37	0X8AD0C2DE	53	0X37E50109
6	0X1EE31FE4	22	0XCD75F47E	38	0X8B90B5D1	54	0X76CE5A8D
7	0X4795C278	23	0XBAECAECB	39	0X21067C87	55	0XEC3B97F0
8	0X266079F6	24	0X5CBBDE55	40	0XDA8CA2C9	56	0X3955610F
9	0XEF36474A	25	0X96C13020	41	0X436A1914	57	0XA0BCA6E3
10	0XFB36A20F	26	0X904C07A0	42	0X64FBD83C	58	0XA3A23D53
11	0X224F7C93	27	0X59BA9BFE	43	0X9F91E54A	59	0X05574025
12	0XB3F9B68B	28	0X0524E56C	44	0X2D377C7E	60	0X52E80B95
13	0XD860D917	29	0X3BFE8389	45	0X148D2FA8	61	0X6E225836
14	0X845A68D1	30	0X7A8F9817	46	0XB10D83E2	62	0X0F74E628
15	0X1EA315A4	31	0X85196862	47	0X7278DA7D	63	0XD9CE3DCB

1507

INDEX	VALUE	INDEX	VALUE	INDEX	VALUE	INDEX	VALUE
0	0X12C0972D	16	0XEFB9FB9E	32	0X745329D2	48	0XB96EC2A5
1	0X4BB64AB1	17	0X9820A12B	33	0XDE05E084	49	0X239B0FD8
2	0X215E71E8	18	0X9407A803	34	0XDF85978B	50	0X62B0545C
3	0X8DCB1F7D	19	0X379D66C6	35	0X821C4AE1	51	0XC976913F
4	0XA82DEA5A	20	0X35D25460	36	0X9DFAD6E4	52	0XE3A1AB09
5	0X145894E7	21	0XF287089C	37	0X4B337B1E	53	0X9D44C5A3
6	0X5688BF84	22	0XF97103B9	38	0XA846E137	54	0X0E1C3ECA
7	0XBAF27918	23	0X6C44D56F	39	0X158F1C42	55	0XA0EAA2F5
8	0X4BF640F1	24	0XD04C3D37	40	0X272D8F28	56	0X8C9B689E
9	0XD10F3D84	25	0X2FDACE42	41	0XE458D6B7	57	0X5A21B37D
10	0X8D358C42	26	0X6EABD6DC	42	0X41D87AFD	58	0X3B770D63
11	0XE6ACE3DE	27	0X5071B039	43	0X7862292B	59	0X07BD5EC0
12	0X771A29C6	28	0X0CEFCEAB	44	0XCAC4B01F	60	0X50021570
13	0XAE63F75A	29	0XC51952F5	45	0X31AE8D69	61	0XF6F76806
14	0XBA63121F	30	0XC3946575	46	0X163F4C41	62	0XF5E9F3B6
15	0X73352CA3	31	0X09EE8B00	47	0X8FD9F79C	63	0X6C00345A

US 2006/0280306 A1

FIG. 58

1602

INDEX	VALUE	INDEX	VALUE	INDEX	VALUE	INDEX	VALUE
0	0X12C0972D	16	0XEFB9FB9E	32	0X745329D2	48	0XB96EC2A5
1	0X4BB64AB1	17	0X9820A12B	33	0XDE05E084	49	0X239B0FD8
2	0X215E71E8	18	0X9407A803	34	0XDF85978B	50	0X62B0545C
3	0X8DCB1F7D	19	0X379D66C6	35	0X821C4AE1	51	0XC976913F
4	0XA82DEA5A	20	0X35D25460	36	0X9DFAD6E4	52	0XE3A1AB09
5	0X145894E7	21	0XF287089C	37	0X4B337B1E	53	0X9D44C5A3
6	0X5688BF84	22	0XF97103B9	38	0XA846E137	54	0X0E1C3ECA
7	0XBAF27918	23	0X6C44D56F	39	0X158F1C42	55	0XA0EAA2F5
8	0X4BF640F1	24	0XD04C3D37	40	0X272D8F28	56	0X8C9B689E
9	0XD10F3D84	25	0X2FDACE42	41	0XE458D6B7	57	0X5A21B37D
10	0X8D358C42	26	0X6EABD6DC	42	0X41D87AFD	58	0X3B770D63
11	0XE6ACE3DE	27	0X5071B039	43	0X7862292B	59	0X07BD5EC0
12	0X771A29C6	28	0X0CEFCEAB	44	0XCAC4B01F	60	0X50021570
13	0XAE63F75A	29	0XC51952F5	45	0X31AE8D69	61	0XF6F76806
14	0XBA63121F	30	0XC3946575	46	0X163F4C41	62	0XF5E9F3B6
15	0X73352CA3	31	0X09EE8B00	47	0X8FD9F79C	63	0X6C00345A

INDEX	VALUE
THE 1ST DATA FOR DISTURBING	0X1C71C71C71C7
THE 2ND DATA FOR DISTURBING	0X55555555